

# EUROPEAN PATENT OFFICE

## Patent Abstracts of Japan

PUBLICATION NUMBER : 10142340  
PUBLICATION DATE : 29-05-98

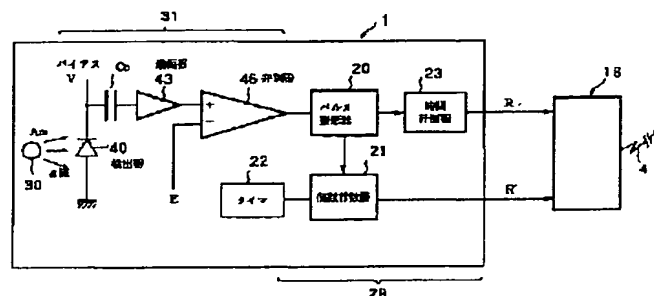
APPLICATION DATE : 08-11-96  
APPLICATION NUMBER : 08296312

APPLICANT : TSUYUSAKI NORIHEI;

INVENTOR : TSUYUSAKI NORIHEI;

INT.CL. : G01T 1/17 G01T 1/30 G06F 7/58  
G09C 1/00

TITLE : RANDOM NUMBER GENERATOR AND  
ENCRYPTION UNIT



ABSTRACT : PROBLEM TO BE SOLVED: To generate an undecodable encryption code by employing numeric values obtained by counting the discharging interval or number of faint radiation as natural random number.

SOLUTION: A shaped pulse signal is delivered from a pulse shaper 20 to a counter 21 which is set with a time interval (t) by a timer 22. The counter 21 counts the shaped pulse signals over the range of time interval (t) and outputs the count as a random number  $R_n$ . Shaped pulse signals from the pulse shaper 20 are also delivered to a time measuring unit 23 and the number of time pulses counted by the time measuring unit 23 before arrival of the shaped pulse is outputted as a random number  $R_t$ . An encryption unit 16 measures the radiation pulses discharged at random through natural decay directly and uses the number of measured pulses and the pulse interval, respectively, as random numbers  $R_n$ ,  $R_t$ . Natural decay of a radioactive substance takes place at random and the time interval for discharging particles is determined and measured at random.

COPYRIGHT: (C)1998,JPO

(51) Int.Cl.<sup>5</sup>  
 G 0 1 T 1/17  
           1/30  
 G 0 6 F 7/58  
 G 0 9 C 1/00  
           6 5 0

F I  
 G 0 1 T 1/17 Z  
           1/30  
 G 0 6 F 7/58 B  
 G 0 9 C 1/00 6 5 0 B

審査請求 未請求 請求項の数 2 O L (全 6 頁)

(21) 出願番号 特願平8-296312

(22) 出願日 平成8年(1996)11月8日

(71) 出願人 595122279

露崎 知子

千葉県茂原市早野1820

(71) 出願人 595122268

露崎 典平

千葉県茂原市早野1820

(72) 発明者 露崎 典平

千葉県茂原市早野1820

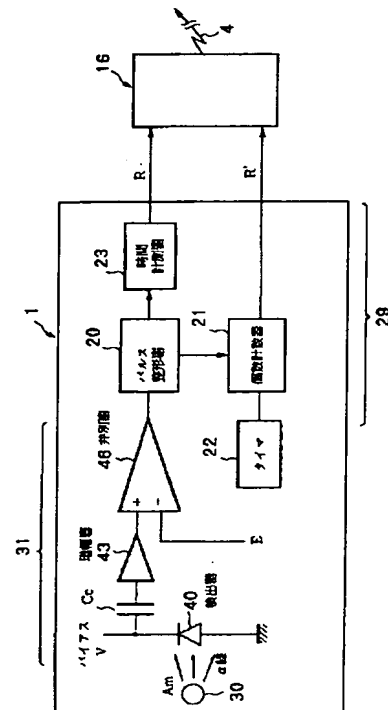
(74) 代理人 弁理士 八嶋 敬市

(54) 【発明の名称】 乱数発生装置と暗号化装置

(57) 【要約】

【課題】 自然から乱数を抽出して、完全に近い乱数を得るとともに、この自然乱数により暗号化を行い解読不能な符号を生成する。

【解決手段】 所定の崩壊常数入に従い、時間 $t$ の経過とともに、放射線を放射して崩壊する微弱な放射性物質を使用し、この放射線の放出間隔を時間の関数として検出し、又は一定時間内の放射線の放出個数を計測し、この計数した数値を乱数として出力する計数回路とする。この乱数に対し特定の有意データを組み合わせて演算を行い暗号を生成する暗号生成回路とを備え、前記乱数とこの暗号データを電磁媒体あるいは光学媒体（赤外線等）を介して離れた位置にある情報処理装置に送り、この情報処理装置では解読回路により前記乱数とこの暗号データに逆演算を行い前記特定の有意データを再生する。



## 【特許請求の範囲】

【請求項1】 所定の崩壊常数 $\lambda$ に従い、時間 $t$ の経過とともに、放射線を放射して崩壊する微弱な放射性物質を使用し、

この放射線の放出間隔を時間の関数として放射線の計数回路で検出し、又は一定時間内の放射線の放出個数を計数回路で計測し、この計数した数値を乱数として情報処理装置に送ることを特徴とする乱数発生装置。

【請求項2】 所定の崩壊常数 $\lambda$ に従い、時間 $t$ の経過とともに、放射線を放射して崩壊する微弱な放射性物質を使用し、

この放射線の放出間隔を時間の関数として検出し、又は一定時間内の放射線の放出個数を計測しかつ、この計数した数値を乱数として出力する計数回路と、

この乱数に対し特定の有意データを組み合わせて演算を行い暗号を生成する暗号生成回路とを備え、

前記乱数とこの暗号データを電磁媒体あるいは光学媒体を介して離れた位置にある情報処理装置に送り、この情報処理装置では解読回路により前記乱数とこの暗号データとの間に逆演算を行い前記特定の有意データを再生することを特徴とする暗号化装置。

## 【発明の詳細な説明】

## 【0001】

【発明の属する分野】本発明は微弱な放射性物質を利用する乱数発生装置とその乱数を使用した暗号化装置及び個人認証システムに関する。

## 【0002】

【従来の技術】これまでの暗号化処理の手法は、ホワイトノイズ等を使用して数式処理を行い人工的に乱数を発生させていた。または、特開平8-123669号のように、混合合同法等の手法を使用して、決められた桁数を決められた回数回の加算や乗算、除算を計算機上で、暗号化処理をしていた。

【0003】これは、元になる乱数が人工的に作成されたものであり、また計算により生成されるため、高精度な乱数にならず、繰り返し使用しているうちに同じ関数になってしまい、映像化して観察すると、一定のパターンが規則的に発生するという欠点が知られている。(Ivars Peterso「コンピューター・グラフィックスが開く現代数学ワンダーランド」奥田 晃訳 新曜社)

## 【0004】

【発明が解決しようとする課題】従来の乱数はコンピュータを使用し計算により生成するので、周期性の発生する域の乱数を使用して、決められた回数の符号化処理を行うと、送信途上で盗聴された場合、現在のスピードの向上した計算機を持てれば、短時間に符号が解読されてしまう恐れがあった。本発明では、自然から乱数を抽出して、完全に近い乱数を得るとともに、この自然乱数により暗号化を行い解読不能な符号を生成することを目的にしている。

## 【0005】

【課題を解決するための手段】本発明の請求項1は、所定の崩壊常数 $\lambda$ に従い、時間 $t$ の経過とともに、放射線を放射して崩壊する微弱な放射性物質を使用し、この放射線の放出間隔を時間の関数として放射線の計数回路で検出し、又は一定時間内の放射線の放出個数を計数回路で計測し、この計数した数値を乱数として情報処理装置に送る。請求項2は、所定の崩壊常数 $\lambda$ に従い、時間 $t$ の経過とともに、放射線を放射して崩壊する微弱な放射性物質を使用し、この放射線の放出間隔を時間の関数として検出し、又は一定時間内の放射線の放出個数を計測し、この計数した数値を乱数として出力する計数回路と、この乱数に対し特定の有意データを組み合わせて演算を行い暗号を生成する暗号生成回路とを備え、前記乱数とこの暗号データを電磁媒体あるいは光学媒体（赤外線等）を介して離れた位置にある情報処理装置に送り、この情報処理装置では解読回路により前記乱数とこの暗号データに逆演算を行い前記特定の有意データを再生する。

## 【0006】

## 【発明の実施の形態】

実施の形態1. 次に、本願の第1発明を図1、4、5、6に従って説明する。図6は本発明に係る放射線の自然崩壊による線源強度の減衰の原理を示す図である。天然または人工放射性物質の核種は、 $\alpha$ 、 $\beta$ 、 $\gamma$ 線等を放射して自然崩壊する、その際、各物質固有の所定の崩壊常数に従って崩壊する。相次で、放射される $\alpha$ 、 $\beta$ 、 $\gamma$ 線はランダムな時間間隔で検出される。今 $\alpha$ 線に注目して説明する。例えば、アメリシウム241 ( $^{241}\text{Am}$ )では、 $\alpha$ 線（ヘリウム原子）がある単位時間に $X$ 個放出される（例えば100個/秒等）。しかしながら、ある単位時間に $X$ 個放出されるといっても、自然現象であるため、ある単位時間に $Y$ 個放出される場合、 $Z$ 個放出される場合、全然放出のない場合等があり、ただ長時間計測すれば、ある単位時間に所定個数放出されるという事実である。

【0007】ここで、ある単位時間に平均 $X$ 個放出されるという捉え方を変更して、相次いで放出（検出）される $\alpha$ 線の時間間隔に注目し、先の $\alpha$ 線から後の $\alpha$ 線の放出までの時間の変数の確率的動き、つまり、確率分布をもって、放射の仕方を規定する。この時の時間の変数は各核種固有の所定の崩壊常数 $\lambda$ に従って、常に一定の確率分布に従っていることが、経験則から知られている。このような確率分布は数学理論では到着理論に属し、放射時間間隔 $t$ の $\alpha$ 線崩壊の様子は図6に示すような指数分布によって表される。

【0008】この指数分布を示す関数は式(1)の $F(t) = N_0 \cdot e^{-\lambda t}$ で表される関数である、以下 $t$ 内は指数を示し、 $N_0$ は初期原子数を示す。この $\lambda$ の崩壊常数は、アメリシウム ( $^{241}\text{Am}$ ) の他にもデ

ータや公知の物理法則や実験技術により、現存する核種については完全に知られている。 $\alpha$ 線の放射を検出するには検出時間間隔を測定するよりもある時間帯に放射される $\alpha$ 線の個数を検出するのが簡単である。アメリシウム<sup>241</sup>の崩壊は $\alpha$ 線の放射時間間隔が指数関数 $F$ に合うので、ある時間帯に放射される $\alpha$ 線の個数を検出すればよい。

【0009】放射分布が指数分布を示す関数 $F(t) = N_0 e^{-\lambda t} \sim (1)$

に従う時、任意の時間 $a$ における区間 $h$ 、 $(a, a+h)$ 内に崩壊する $\alpha$ 線の個数が $k$ 個である確率 $P_k$ は、次の式(2)で表示できる。

$P_k = M^{-k} e^{-M} / k! \sim (2)$

ここで $\{ \}$ 内は指数を示し、 $M$ は平均値を示し、 $k!$ は $k$ の階乗である。この分布は図7のポアソン分布であり、時間区間の始点 $a$ に無関係で、その平均値は $M$ である。

【0010】本願発明者は原理を応用して、アメリシウム(<sup>241</sup>Am)(放射性同位元素、以下単にRIと称す)の放射能による乱数を応用して乱数発生装置と暗号化装置を作成した。以下に上記原理による、乱数発生装置と暗号化装置について説明する。まず、図1は乱数発生装置(RPG)1の構成を示し、乱数発生装置(RPG)1は放射性カプセル30と検出装置31と乱数発生回路29とから構成される。放射性カプセル30は、人体に無害な微量の $\alpha$ 、 $\beta$ 、 $\gamma$ 線を放射する、例えば人工の放射性核種(物質、以後RIと称す)のアメリシウム<sup>241</sup>(<sup>241</sup>Am)である。

【0011】この放射性カプセル30から放射される $\alpha$ 線は検出装置31により検出される。この検出装置31はRIからの $\alpha$ 線等を検出し、検出信号を計測装置29に出力する。検出装置31は、RIの $\alpha$ 崩壊により放出される $\alpha$ 粒子をPINダイオードで電流として補足する公知の方法を利用する。

【0012】乱数発生回路29(計測装置)はこれら信号中から所定の放射能( $\alpha$ または、 $\beta$ または、 $\gamma$ 線)による信号のみを選択し、かつ設定された所定の時間 $h$ 以内に計測される信号の個数を計数する。

【0013】更に、検出装置31はPINダイオード40と結合コンデンサCcと前置増幅器43と弁別器46から構成されている。放射性カプセル30にPINダイオード40を対面させて、円筒形の金属筒内に納めて半導体内に $\alpha$ 線源が侵入し易いようにした。

【0014】バイアス電圧VがPINダイオード40に印加され、PINダイオード40はp-n結合の半導体であって、 $\alpha$ 線源が侵入すると不安定電子や不安定正ホールが移動し、いわゆる通電し、PINダイオード40の両端に電流が発生する。

【0015】この変動電流は微弱なもので結合コンデンサCcを介して前置増幅器43に送られ、そこで増幅

され、パルス信号として出力される。弁別器46には、これらパルス信号と基準電圧Eとが送られ、ノイズを分離するため基準電圧Eより大きいパルス及び基準内の信号のみを選択する。即ち、前置増幅器43からは $\alpha$ 線によるパルス信号と他の雑音によるパルス信号が混在しているので、弁別器46により、 $\alpha$ 線によるパルス信号だけを取り出すようにしている。

【0016】この乱数発生装置(RPG)1では、基準電圧Eを適当に設定して、 $\alpha$ 線の放射線によるパルス信号のみを取り出すようにする。今ここでは $\alpha$ 線に注目して、 $\alpha$ 線を放出する<sup>241</sup>Am核種の場合について述べたが、 $\beta$ 線、 $\gamma$ 線についても同様に計測可能である。乱数発生回路29は、パルス整形器20と個数計数器21とタイマ22と時間計測器23とから構成される。放射線によるパルス信号は、乱数発生回路29のパルス整形器20に送られ、以後の計数回路のパルス波計との標準化がなされる。

【0017】パルス整形器20からの整形済パルス信号は個数計数器21に送られ、個数計数器21にはタイマ22から時間間隔 $t$ が設定される。個数計数器21では、図4に示すように設定された時間間隔範囲で整形済パルス信号を計数し、計数値を乱数 $R_n$  : 3, 5, 2, 1...として出力する。単位時間に計測された放射線のパルスのランダムな数値をそのまま乱数 $R_n$ として使用する。

【0018】またパルス整形器20からの整形済パルス信号は時間計測器23に送られ、時間計測器23では時間パルスを計数しているが、図5に示すように整形済パルス信号が到着する時間、時間パルスの数を乱数 $R_t$  : 8, 5, 7...秒(例えば)として出力する。乱数発生装置(RPG)1は、自然崩壊によるランダムに放出される放射線をパルスとして直接計測し、計測されたパルス間隔(時間)を乱数 $R_t$ として使用する。

【0019】放射性物質(RI)の自然崩壊は全くランダムに起こる現象であり、放出される粒子の放出時間の間隔は全くランダムであり、よって計測される時間間隔も全くランダムとなる。今、設定された時間間隔範囲で計数された整形済パルス信号、即ち、単位時間に放射性物質の自然崩壊で計数される乱数 $R_n$ について考察する。

【0020】線源の強度が弱い放射性物質(RI)の自然崩壊で計測される単位時間の $\alpha$ 線数が、 $0 < R_n < 5 \sim 60$ の範囲の場合は、図7のポアソン分布になり、 $\alpha$ 線数が、 $R_n > 5 \sim 60$ の範囲の場合は、図8の左右対称のガウス分布になる。

【0021】得られた計数される乱数 $R_n$ は、どちらの分布でも平均計数値 $M$ を中心にした数値に分布するが、例えば平均計数値 $M=7$ なら7が一番多く、6、8が次に、また5、9がその次に多く計数される。しかしこれら数7、6、8、5、9等の発生順は、全くランダムで

あり、計数値は乱数 $R_n$ として信頼できる。

【0022】乱数発生装置(RPG)1からの乱数 $R_t$ または乱数 $R_n$ は暗号化装置16に送られ、そこで暗号の生成に利用される。さて、RPG1では線源強度を調整することにより、平均的な放出時間を調整することは可能である。崩壊は人工的にコントロールすることは一切できない、よって得られた関数は、全くランダム関数である、人工的に作成されたものではない。

【0023】計測時間、計測個数を8ビット、16ビット、32ビット、64ビットの桁数と対応させて、ビットに対応する数値を乱数として使用できる。また各ビットに対応した0または1を計測するRPGを設置してもよい、この場合は放射線を検出した時1、検出しなかった時0、とすれば線源強度は検出限界まで、低下させることができる。ランダムに得られる時間の数値、あるいは単位時間に計測されるパルスの数値をそのまま乱数として、使用する。

【0024】次に、図2、3において、第2発明の暗号化装置16を説明する。暗号化装置16は、送信側は前述の乱数発生装置(RPG)1と暗号生成回路2と規則決定部10と演算種テーブル13と送信回路3とから構成される。乱数発生装置(RPG)1からの乱数 $R$ は、規則決定部10と暗号生成回路2に送られ、暗号生成回路2には特定の有意データ $S$ も送られてくる。

【0025】演算種テーブル13は演算種を予め記憶し、規則決定部10は乱数と有意データとの間でどのような演算を実行するのかを、乱数に基づき演算種テーブル13を参照して暗号生成回路2に指定する。

【0026】規則決定部10は乱数発生装置(RPG)1からの乱数 $R$ に従い、演算種テーブル13から、初期値が奇数なら加算、偶数なら減算、或は実数の0なら乗算、1なら除算、2なら自乗・・・等の演算種 $Z$ を読み出し、暗号生成回路2に指令する。

乱数 $R$	75354378	93244831	46367489	...
有意データ $S$	1	2	3	...
暗号データ $RS$	75354379	93244833	46367482	
混合信号 $R, RS$	75354378	75354379		
	93244831	93244833		
	46367489	46367481		

【0033】受信側 乱数 $R$ 75354378の先頭が7(奇数)だから規則1の逆算に決定。

暗号データ $RS$	75354379	93244833	46367482
乱数 $R$	-75354378	93244831	46367489
有意データ $S$ (差)	1	2	3

注: 46367482-46367489では、各桁は独立とし、不足したら、その桁にのみ10を加えたものから引く、2-9では10+2-9=3とする。

【0034】加算の場合:  $R+S=RS$ 、規則1: 各桁  
乱数 $R$             4桁

【0027】暗号生成回路2では、この乱数 $R$ に対し特定の有意データを、例えば加算し暗号信号 $RS$ として送信回路3に出力する。送信回路3には、乱数発生装置(RPG)1からの乱数 $R$ も送られており、送信回路3は、乱数 $R$ とこの暗号データ $RS$ を混合信号 $R, RS$ として、電磁媒体の通信回線4や電波及び光学媒体(赤外線等)を介して離れた位置にある図3の情報処理装置8に送る。

【0028】図3の受信側では、情報処理装置8は、分離回路5と解読回路6と情報処理部7と規則再現部11と逆演算種テーブル12とから構成される。通信回線4からの混合信号 $R, RS$ は、分離回路5により乱数 $R$ と暗号データ $RS$ とに分離され、分離された乱数 $R$ とこの暗号データ $RS$ は解読回路6に別々に入力され、分離された乱数 $R$ は規則再現部11に送られる。

【0029】逆演算種テーブル12には、演算種テーブル13の奇数なら加算、偶数なら減算、或は実数の0なら乗算、1なら除算、2なら自乗・・・等の演算種 $Z$ に対応して、逆演算種 $-Z$ の一覧を予め格納している。

【0030】乱数 $R$ は規則再現部11に送られ、規則再現部11は乱数 $R$ の初期値を参照して、逆演算種テーブル12から受信した演算種 $Z$ の逆演算種 $-Z$ を読み出し、解読回路6に送る。解読回路6では、逆演算種 $-Z$ に従い、暗号データ $RS$ から乱数 $R$ を減算、逆演算を行い、特定の有意データ $S$ を再生する。

【0031】有意データ $S$ は情報処理部7に送られ、電子取り引きや、株取り引き、セキュリティコード、秘密情報の伝達等に利用される。さて、暗号化の各種方法について説明する。送信側では、乱数 $R$ 75354378の初期値、先頭が7(奇数)なら演算を規則1に決定。

【0032】加算の場合:  $R+S=RS$ 、規則1: 各桁を加算するが桁上りはしない。

減算の場合:  $RS-R=S$ 、規則2: 各桁を減算するが上位桁から引かない。

を加算するが桁上りはしない。

送信側 乱数 $R$ 3725の初期値、先頭が3(奇数)なら演算を規則1に決定。

3727

有意データS 4桁  
暗号データRS 4桁  
混合信号R、RS 通信回路上のデータ

【0035】受信側 乱数R 3727の先頭が3(奇数)だから規則1の逆算に決定。

暗号データRS  
乱数R  
有意データS(差)

注: 7802-3727では、各桁は独立とし、不足したら、その桁にのみ10を加えたものから引く、0-2では10+0-2=8とする。

【0036】この発明では、完全乱数でデータを暗号化し、かつ演算種テーブル13(逆演算種テーブル12)を乱数0、1、2、3、4、5、6、7、8、9や偶数、奇数等毎に、予め送信側と受信側で決定しておいて使い分けるので、データの都度演算種を自動発生することができ、完全な暗号に近くなり、第三者による盗聴や解読が不可能になる。

【図面の簡単な説明】

【図1】本発明の乱数発生装置の一実施例を示す回路のブロック図である。

【図2】本発明の暗号化装置の送信側の一実施例を示す回路のブロック図である。

【図3】本発明の暗号化装置の受信側の一実施例を示す回路のブロック図である。

【図4】単位時間に計測されるランダムパルスの数値を示す図である。

【図5】本発明の乱数発生装置からランダムに得られる時間値を示す図である。

【図6】本発明に利用する崩壊現象を示す指数関数の図である。

【図7】一般的なポアソン分布のグラフ図である。

【図8】一般的なガウス分布のグラフ図である。

【符号の説明】

- 1 乱数発生装置  
2 暗号生成回路

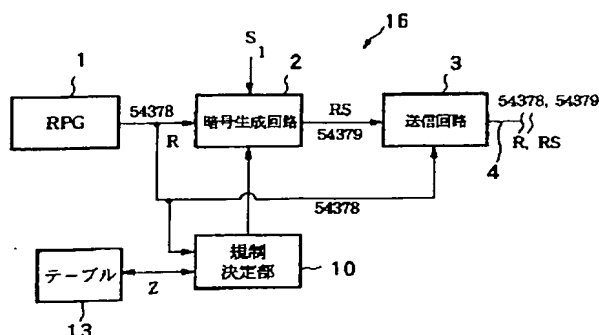
+4185  
7802  
3727 7802

減算の場合: RS-R=S、規則2: 各桁を減算するが上位桁から引かない。

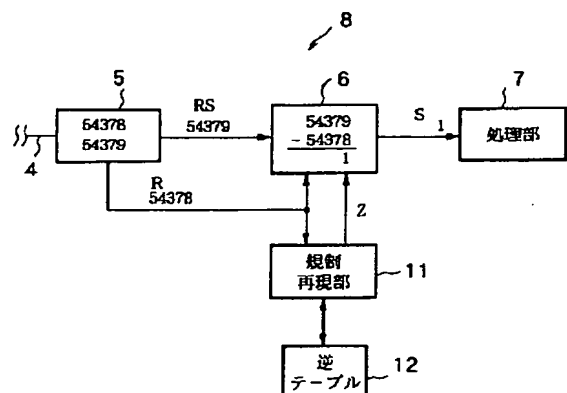
7802  
-3727  
4185

- 3 送信回路  
4 通信回線  
5 分離回路  
6 解読回路  
7 情報処理部  
8 情報処理装置  
10 規則決定部  
11 規則再現部  
12 逆演算種テーブル  
13 演算種テーブル  
16 暗号化装置  
21 個数計数器  
22 タイマ  
23 時間計測器  
29 乱数発生回路  
30 放射性カプセル  
31 検出装置  
32 計測装置  
40 PINダイオード  
43 前置増幅器  
46 弁別器  
Cc 結合コンデンサー  
E 基準電圧  
R、RS 混合信号  
R 乱数  
RS 暗号データ  
S 有意データ  
V バイアス電圧

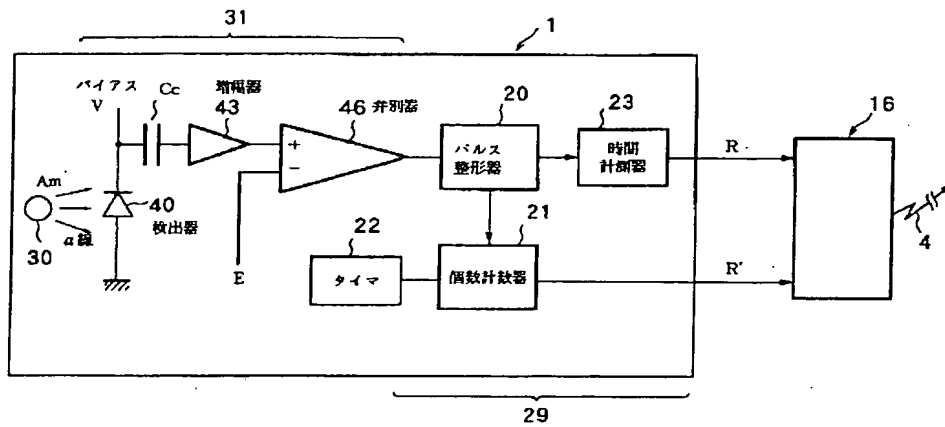
【図2】



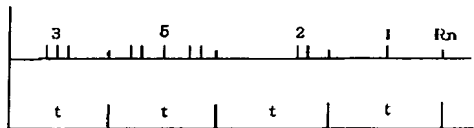
【図3】



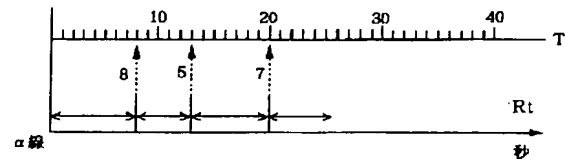
【図1】



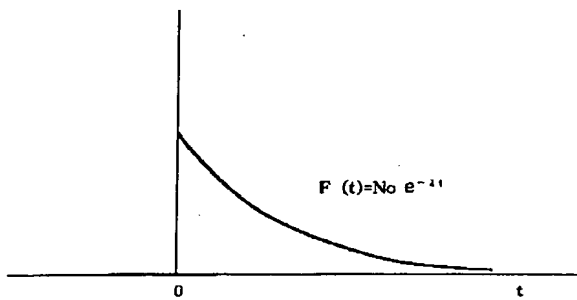
【図4】



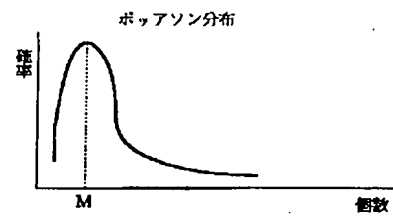
【図5】



【図6】



【図7】



【図8】

